REMARKS

[0007] Applicant respectfully requests reconsideration and allowance of all of the claims of the application. Claims 1, 3-8, 10-15 and 24-26 are presently pending. Claims 3-8, 10-15 and 24-26 are amended herein. No claims are withdrawn or canceled herein. No new claims are added herein.

Formal Request for an Interview

[0008] If the Examiner's reply to this communication is anything other than allowance of all pending claims and there only issues that remain are minor or formal matters, then I formally request an interview with the Examiner. I encourage the Examiner to call me—the undersigned representative for the Applicant—so that we can talk about this matter so as to resolve any outstanding issues quickly and efficiently over the phone.

[0009] Please contact me to schedule a date and time for a telephone interview that is most convenient for both of us. While email works great for me, I welcome your call as well. My contact information may be found on the last page of this response.

Claim Amendments

[0010] Without conceding the propriety of the rejections herein and in the interest of expediting prosecution, Applicant amends claim 24 herein. Applicant amends this claim to highlight claimed features. Such amendments are made to expedite prosecution and more quickly identify allowable subject matter. Such amendments are merely intended to highlight the claimed features, and should not be construed as further limiting the claimed invention in response to the cited reference.

[0011] Support for the amendments to claim 24 is found in Figures 3 and 4 and their corresponding discussion in the specification.

Substantive Matters

Claim Rejections under § 112 2nd ¶

[0012] Claims 3, 4, 5-7 and 10-12 are rejected under 35 U.S.C. § 112, 2nd ¶. Applicant respectfully traverses this rejection. Furthermore, in light of the amendments presented herein, Applicant submits that these rejections are moot. Accordingly, Applicant asks the Examiner to withdraw these rejections.

Claim Rejections under § 101

[0013] Claims 8 and 10-15 are rejected under 35 U.S.C. § 101. Applicant respectfully traverses this rejection. Furthermore, in light of the amendments presented herein, Applicant submits that these rejections are moot. Applicant herein submits that that the claims of the instant Application are to be construed—now and in the future--to be limited to subject matter deemed patentable in accordance with United States Federal statutes, namely section 101 of Title 35 U.S.C., and as interpreted by appropriate and authoritative Article III entities. Accordingly, Applicant asks the Examiner to withdraw these rejections.

[0014] If the Examiner maintains the rejection of these claims, then Applicant requests additional guidance as to what is necessary to overcome the rejection.

Claim Rejections under § 102

[0015] The Examiner rejects claims 1, 3-8, 10-15,24-26 under § 102. For the reasons set forth below, the Examiner has not shown that the cited reference anticipates the rejected claims. Accordingly, Applicant respectfully requests that the § 102 rejections be withdrawn and the case be passed along to issuance.

[0016] The Examiner's rejections are based upon **van der Made:** *van der Made, et al.*, US Patent No. 7,093,239 (issued August 15, 2006).

Overview of the Application

[0017] The Application describes facilitating the adoption and recognition by an operating system of an otherwise unsupported executable-image format by increasing the ease with which an executable-image loader may be modified.

Cited Reference *van der Made*

[0018] *van der Made* describes an automated analysis system that detects malicious code within a computer system by generating and subsequently analyzing a behavior pattern for each computer program introduced to the computer system. Generation of the behavior pattern is accomplished by a virtual machine invoked within the computer system. An initial analysis may be performed on the behavior pattern to identify infected programs on initial presentation of the program to the computer system. The analysis system also stores behavior patterns and sequences with their corresponding analysis results in a database. Newly infected programs can be detected by analyzing a

newly generated behavior pattern for the program with reference to a stored behavior pattern to identify presence of an infection or payload pattern.

Anticipation Rejections

[0019] Applicant submits that the anticipation rejections are not valid because, for each rejected claim, no single reference discloses each and every element of that rejected claim.[1] Furthermore, the elements disclosed in the single reference are not arranged in the manner recited by each rejected claim.[2]

Based upon van der Made

[0020] The Examiner rejects claims 1, 3-8, 10-15 and 24-26 under 35 U.S.C. § 102(e) as being anticipated by van der Made. Applicant respectfully traverses the rejection of these claims. Based on the reasons given below, Applicant asks the Examiner to withdraw the rejection of these claims.

---

[1] "A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." Verdegaal Bros. v. Union Oil Co. of California, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987); "The identical invention must be shown in as complete detail as is contained in the ... claim." *Richardson v. Suzuki Motor Co.*, 868 F.2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989); also see MPEP §2131.

[2] See *In re Bond*, 910 F.2d 831, 15 USPQ2d 1566 (Fed. Cir. 1990).

Independent Claim 1

[0021] Applicant submits that van der Made does not anticipate this claim because it does not disclose at least the following features as recited in this claim (with emphasis added):

> "a file-format recognizer, configured to recognize the file format of the executable image from amongst a database of multiple file format definitions, wherein the ***database is extensible so that additional file format definitions may be added to the database of multiple file format definitions***;"

[0022] The Examiner indicates (Action, p. 4-5) the following with regard to this claim:

Regarding claim 1, Van discloses: A computer-readable medium having computer-executable modules comprising:

a file locator configured to locate an executable image on a computer media (i.e., search for the first EXE file in this directory... see col. 10, lines 33-45, Van);

a file format recognizer , configured to recognize the file format of the executable image from amongst a database of multiple file format definitions (see col. 8, lines 26-36, Van), wherein the database is extensible so that additional file format definitions may be added to the database of multiple file format definitions (see col. 7, lines 33 to col. 8, lines 25, and database of executables fig. 2, Van).

a memory-mapper configured to open the executable image from the computer media and read it into a computer memory (i.e., the file is opened and the virtual machine reads the relevant code into memory as a data stream... a memory mapping utility maps the virtual memory map to the offset of the file type that is virtualized... see col. 9, lines 2-10, Van);

an importer configured to find a list of executable image names to load (i.e., a memory mapping utility maps the virtual memory map to the offset for the file type that is virtualized, such as binary image files, executable format files document files... see col. 9, lines 10-25, Van);

an exporter configured to build a representation of program modules that an executable image exports (i.e., see col. 8, lines 61-87, Van);

a binder configured to link multiple executable images together, such images being those of the list of executable image names (i.e., compound document files can contain executable streams, such as fig. 3, file contains a linked list which is referenced in a directory structure that points to the entry point of the linked list... see col. 8, lines 37-44, Van);

[0023] The Examiner appears to equate the different file formats as described in van der Made to the extensible database as specified in claim 1. Applicant respectfully disagrees.

[0024] Van der Made is directed towards identifying the presence of malicious code in program code within a computer system, including initializing a virtual machine within the computer system. The initialized virtual machine comprises software simulating functionality of a central processing unit and memory. The virtual machine virtually executes a target program so that the target program interacts with the computer system only through the virtual machine. The system analyzes the behavior of the target program following virtual execution to identify occurrence of malicious code behavior and indicate in a behavior pattern the occurrence of the malicious code behavior. (van der Made Col. 2 Lines 50-61)

[0025] Van der Made further describes that before the program can be virtualized, the file format containing the target program has to be evaluated. The entry point code is extracted and loaded into the virtual computer's memory at the correct simulated offset. In a physical computer this function would be performed by the program loader function, which is part of the operating system. The operating system can execute programs that are held in a collection of different file formats. (van der Made Col. 7 Lines 42-48) Van der Made then lists the different file formats that are supported by the operating systems in Columns 7-8. However, this list is a set list, such that the different file formats listed are supported by the operating system described in van der Made.

[0026] Thus, van der Made does not disclose, teach or suggest "wherein the ***database is extensible so that additional file format definitions may be added to the database of multiple file format definitions"*** as recited in claim 1. Instead, van der Made lists file formats that are supported by the operating system.

[0027] Consequently, van der Made does not disclose all of the elements and features of this claim. Accordingly, Applicant asks the Examiner to withdraw the rejection of this claim.

Dependent Claims 3-7

[0028] These claims ultimately depend upon independent claim 1. As discussed above, claim 1 is allowable over the cited reference. It is axiomatic that any dependent claim which depends from an allowable base claim is also allowable over the cited reference at least for the same reason(s) its base claim is allowable. Additionally, some or all of these claims may also be allowable for additional independent reasons.

Independent Claim 8

[0029] Applicant submits that van der Made does not anticipate this claim because it does not disclose at least the following features as recited in this claim (with emphasis added):

> "***a database of multiple executable-image formats*** which is the basis for which the recognizer recognizes the format of executable image and for which the memory-mapper varies how it loads and maps the executable image into memory, ***wherein the database is extensible so that additional executable-image formats may be recognized by the recognizer and loaded and mapped by the memory-mapper,***"

[0030] Similar to the explanation given above with respect to claim 1, it appears the Examiner is equating the list of supported file formats as disclosed in van der Made to an extensible database as recited in the claims. While van der Made discloses a list of file formats supported by an operating system, van der Made does not disclose, teach or suggest a database that is "*extensible so that additional executable-image formats may be recognized by the recognizer and loaded and mapped by the memory-mapper*," as recited in claim 8.

[0031] Consequently, van der Made does not disclose all of the elements and features of this claim. Accordingly, Applicant asks the Examiner to withdraw the rejection of this claim.

Dependent Claims 10-15

[0032] These claims ultimately depend upon independent claim 8. As discussed above, claim 8 is allowable over the cited reference. It is axiomatic that any dependent claim which depends from an allowable base claim is also allowable over the cited reference for at least the same reason(s) its base claim is allowable. Additionally, some or all of these claims may also be allowable for additional independent reasons.

Independent Claim 24

[0033] Applicant submits that van der Made does not anticipate this claim because it does not disclose at least the following features as recited in this claim (with emphasis added):

"A computer implemented method facilitating loading of one or more executable images of varying formats, the method comprising:

locating an executable image on a computer-readable storage media;

investigating information related to the executable image, thereby identifying the format of the executable image, wherein:

during the investigating, accessing ***an extensible database of executable-image formats***; and

the investigating accesses a header of the executable image in order to identify the format;

initiating an extensible loader associated with the identified format, wherein ***the extensible loader***:

is pointed to by an entry; and

comprises a plurality of modules that are selectively combined to accommodate executable image formats not supported by a native operating system, each module including at least one component designed for a specific executable image format;

loading the executable image into a computer memory using ***the extensible loader***, wherein the loading comprises:

calling an entry point located in loaded program libraries in order to load the executable image;

creating a new process based on the entry point;

creating necessary sections within the loaded program libraries for the executable image;

creating an initial thread for the executable image; and

handing over control from the ***extensible loader*** to the initial thread in order to execute the executable image."

[0034] The Examiner indicates (Action, p. 7-8) the following with regard to this claim:

Regarding claim 24, Van disclose: a computer implemented method facilitating loading of one

or more executable images of varying formats, the method comprising: locating an executable image on a computer media (search for the first EXM file in this directory... see paragraph col. 10, lines 33-34, Van);

investigating information related to the executable image, thereby identifying the format of the executable image, wherein: during the investigating, accessing an extensible database of executable-image formats (i.e., the file structure analysis procedure looks in the file header and file structure to determine the file format... see coll. 8, lines 30-33 and the program code is checked against the database for known files, if the file is new or modified, it is processed, the resulting behavior signature is

analyzed or compared and stored... see col. 7, lines 32 to col. 8, lines 20; and col. 11, lines 8-30, Van); and

the investigating accesses a header of the executable image in order to identify the format (i.e., the file structure analysis procedure looks in the file header and file structure to determine the file format... see coll. 8, lines 30-33, Van);

initiating an extensible loader associated with the identified format, the extensible loader being pointed to by an entry (see col. 7, lines 41-46, Van);

loading the executable image into a computer memory using the extensible loader, wherein the loading (see col. 8, lines 25-36, Van) comprises:

calling an entry point located in loaded program libraries in order to load the executable image (col. 7, lines 42-56, Van);

creating a new process based on the entry point (col. 9, lines 1-8, Van);

creating necessary sections within the loaded program libraries for the executable image (see col. 7, lines 46-48, Van);

creating an initial thread for the executable image (see col. 9, lines 38-42, Van); and

handing over control from the extensible loader to the initial thread in order to execute the executable image (see l. 10, lines 5-14, Van).

[0035] In addition to the reasons explained above with respect to claims 1 and 8, Applicant submits that van der Made does not anticipate this claim because van der Made does not disclose "***a plurality of modules that are selectively combined to accommodate executable image formats not supported by a native operating system.***"

[0036] Van der Made does not disclose, teach or suggest selectively combining a plurality of modules because van der Made is limited to listing file formats that are supported by the operating system described in van der Made. Thus, van der Made does not disclose, teach or suggest a situation where an unsupported a file format is identified.

[0037] Consequently, Van der Made does not disclose all of the elements and features of this claim. Accordingly, Applicant asks the Examiner to withdraw the rejection of this claim.

Dependent Claims 25-26

[0038] These claims ultimately depend upon independent claim 24. As discussed above, claim 24 is allowable over the cited reference. It is axiomatic that any dependent claim which depends from an allowable base claim is also allowable over the cited reference for at least the same reason(s) its base claim is allowable. Additionally, some or all of these claims may also be allowable for additional independent reasons.

Dependent Claims

[0039] In addition to its own merits, each dependent claim is allowable for the same reasons that its base claim is allowable. Applicant requests that the Examiner withdraw the rejection of each dependent claim where its base claim is allowable.

Conclusion

[0040] All pending claims are in condition for allowance. Applicant respectfully requests reconsideration and prompt issuance of the application. If any issues remain that prevent issuance of this application, the **Examiner is urged to contact me before issuing a subsequent Action**. Please call or email me at your convenience.

Respectfully Submitted,

Lee & Hayes, PLLC
Representatives for Applicant

/Jacob Rohwer 61,229/ Dated: 1/27/2009
Jacob P. Rohwer (jacob@leehayes.com; 206-876-6004)
Registration No. 61,229
Bea Koempel-Thomas (bea@leehayes.com; 509-944-4759)
Registration No. 58,213
Customer No. **22801**

Facsimile: (509) 323-8979
www.leehayes.com